Listing of Claims (replaces all previous versions):

1. (currently amended) A system for establishing communications across a firewall comprising:

a communications network;

a first server within said communications network;

a first computer separated from said communications network, said first computer sending information to said first server; and,

a second computer separated from said communications network, said second computer receiving information from said first server related to the information sent from said first computer,

wherein at least one of said first computer and said second computer are separated from said communications network by at least one firewall,

wherein said first computer transmits a hypertext transfer protocol (HTTP) message to said first server with an encrypted identification of said second computer,

wherein said first server decrypts said encrypted identification to an unencrypted identification of said second computer and forwards said message to said second computer using said unencrypted identification,

wherein said HTTP message is transmitted through a firewall port that is normally open ~~by default~~ to HTTP packets ~~Internet traffic~~.

2. (previously presented) The system according to claim 1, wherein said first computer transmits said message to said first server with encrypted message content and said server transmits said encrypted message content to said second computer without decrypting said message in said server.

3. (Cancelled)

4. (currently amended) The system according to claim 1, wherein said first computer further includes a first client and said second computer includes a second client and wherein each of said first client and said second client use an open firewall port that is normally open ~~by default~~ to HTTP packets ~~Internet traffic~~ to access said communications network.

5. (Original) The system according to claim 4, wherein said open port is at least one of port 80 and port 8080.

6. (Original) The system according to claim 1, further comprising a second server that operates in the event of an error with said first server.

7. (Original) The system according to claim 1, wherein the information received at said second computer has the same content as the information sent from said first computer.

8. (Original) The system according to claim 1, wherein the information received at said second computer has different but related content as the information sent from said first computer.

9. (Original) The system according to claim 1, further comprising

a second server, said second server being connected to said network,

wherein said second server replaces said first server when an error occurs between said first server and at least one of said first computer and said second computer.

10. (Original) The system according to claim 1, further comprising

a second server, said second server being connected to said network,

wherein said second server replaces said first server when an error occurs with said first server.

11. (Original) The system according to claim 1, further comprising:

at least a third computer,

wherein at least said third computer receives information from said first server related to the information sent from said first computer,

wherein at least said third computer is separated from said communication network by at least one of said first or at least a second firewall.

12. (Original) The system according to claim 1, wherein a communication pathway between said first server and at least one of said first computer and said second computer is kept open by repeated transmissions from said first server.

13. (Original) The system according to claim 1, wherein a communication

pathway between said first server and at least one of said first computer and said second computer is kept open by repeated transmissions from at least one of said first computer and said second computer.

14. (Cancelled)

15. (previously presented)The system according to claim 1, wherein said first computer transmits said message to said first server with a header, the header including at least one of an encrypted header, an encrypted identification, an encrypted IP address, an encrypted username of said second computer, an encrypted size, an encrypted CRC, an encrypted header length, an encrypted message length, an encrypted asset identifier, an encrypted name of at least one client, and an encrypted application ID, an encrypted time and date stamp, an encrypted location ID, an encrypted message types, an encrypted attachment identifier, an encrypted packet number, and an encrypted pre-compressed data size for an associated message.

16-18. (Canceled)

19. (previously presented)A method for transmitting information across a network comprising the steps of:

receiving an encrypted identification of a second computer from a first computer;

receiving an encrypted message from said first computer;

decrypting said encrypted identification into an unencrypted identification of said second computer; and,

transmitting said encrypted message to said second computer without decrypting said encrypted message,

wherein at least one of said receiving steps and said transmitting step includes receiving or transmitting through a firewall port that is normally open by default to Internet traffic.

20. (Original) The method according to claim 19, wherein said encrypted message is also compressed.

21. (previously presented) A computer-readable medium storing a program for transmitting information across a network, said program comprising the steps of:

receiving an encrypted identification of a second computer from a first computer;

receiving an encrypted message from said first computer;

decrypting said encrypted identification into an unencrypted identification of said second computer; and

transmitting said encrypted message to said second computer without decrypting said encrypted message,

wherein at least one of said receiving steps and said transmitting step includes receiving or transmitting through a firewall port that is normally open by default to Internet traffic.

22. (Original) The computer readable medium according to claim 21, wherein said encrypted message is also compressed.

23. (Canceled)

24. (previously presented)A method for transmitting information across a network comprising the steps of:

encrypting an identification of a second computer at a first computer;

encrypting a message such that said message can only be decrypted by said second computer; and

transmitting to a server said encrypted identification and said encrypted message, wherein said server later decrypts said encrypted identification and transmits said encrypted message to said second computer,

wherein at least one of said first computer and said second computer are separated from the server by a firewall and wherein said encrypted message is transmitted through a port on the firewall that is normally open by default to Internet traffic .

25. (Canceled)

26. (previously presented)A computer readable medium storing a program for transmitting information across a network, said program comprising the steps of:

encrypting an identification of a second computer at a first computer;

encrypting a message such that said message can only be decrypted by said second computer; and

transmitting to a server said encrypted identification and said encrypted message, wherein said server later decrypts said encrypted identification and transmits said encrypted message to said second computer,

wherein at least one of said first computer and said second computer are separated from said server by a firewall and wherein said encrypted message is transmitted through a port on the firewall that is normally open by default to Internet traffic.

27. (previously presented)A system for transmitting information between a first computer and a second computer comprising:

a first application; and

a first computer hosting a first client, said first client receiving data from said first application, said first computer transmitting said data to a server, said server forwarding said data to a second client residing on said second computer, said second client forwarding said data to at least a second application,

wherein at least one of said first computer and said second computer are separated from said server by a firewall,

wherein said first computer transmits a message to said server with an encrypted identification of said second computer, said message being encrypted for decryption at said second client, and

wherein said server decrypts said encrypted identification to an unencrypted identification of said second computer and forwards said encrypted message to said second computer using said unencrypted identification, and

wherein one of said encrypted message transmitted from said first computer and said encrypted message forwarded to said second computer are transmitted through a firewall port that is normally open by default to Internet traffic.

28. (Original) The system according to claim 27, wherein said first application is hosted by a third computer that communicates with said first computer.

29. (Original) The system according to claim 27, wherein said first application is hosted by said first computer.

30. (Previously Presented) The system according to claim 27, wherein said second application is hosted by a third computer that communicates with said second computer.

31. (Previously Presented) The system according to claim 27, wherein said second application is hosted by said second computer.

32. (Original) The system according to claim 27, wherein said first computer transmits said data as encrypted data and said server transmits said encrypted data to said second computer.

33. (Cancelled)

34. (Original) The system according to claim 27, wherein said first computer and said second computer each use an open port to access to said communications network.

35. (Original) The system according to claim 34, wherein said open port is at least one of port 80 and port 8080.

36. (Original) The system according to claim 27, wherein said first client communicates with said first application by an application programming interface.

37. (Original) The system according to claim 27, wherein said first client communicates with said first application by a proxy.

38. (Original) The system according to claim 27, wherein said first client communicates with said first application by sockets.

39-44. (Canceled)

45. (previously presented)A computer-readable medium storing a program for transmitting information across a network between a first computer and a second computer, said network including a server that has received and decrypted an encrypted identification of said second computer, said server having transmitted an encrypted message to said second computer using said decrypted identification, said encrypted message having been encrypted at said first computer for decrypting at said second computer, said program comprising the steps of:

receiving at said second computer from said server said encrypted message and a header with encrypted information;

decrypting said encrypted information; and

decrypting said encrypted message,

wherein at least one of said first computer and said second computer are separated from said server by a firewall and said encrypted message is transmitted through a firewall port that is normally open by default to Internet traffic.

46. (previously presented)The computer readable medium according to claim 45, wherein said header includes at least one of an encrypted identification, an encrypted IP address, an encrypted username of said second computer, an encrypted size, an encrypted CRC, an encrypted header length, an encrypted message length, an encrypted asset identifier, an encrypted name of at least one client, and an encrypted application ID, an encrypted time and date stamp, an encrypted location ID, an encrypted message types, an encrypted attachment identifier, an encrypted packet number, and an encrypted pre-compressed data size for an associated message.

47. (previously presented) A method of transferring data between a first computer and a second computer coupled over a network, comprising the steps of:

(1) receiving a first hypertext transfer protocol (HTTP) message containing information intended for delivery to the second computer, wherein the first message is received through a first firewall associated with the first computer through a port that is normally open by default to Internet traffic;

(2) receiving a second hypertext transfer protocol (HTTP) message from the second computer, wherein the second message causes a return path to be established to the second computer and is received through a second firewall associated with the second computer through a port that is normally open by default to Internet traffic; and

(3) transmitting to the second computer via the return path contents of the first message received from the first computer.

48. (previously presented) The method of claim 47, wherein the first and second HTTP messages each comprise an HTTP POST message.

49. (currently amended) The method of claim 47, wherein steps (1) through (3) are performed on an intermediate server computer that is separate from the first computer and the second computer and located between the first and second firewalls.

50. (previously presented) The method of claim 49, wherein in step (1), the first message received from the first computer is encrypted by the first computer, and wherein in step (3), the third computer transmits encrypted message content received from the first computer to the second computer via the return path.

51. (previously presented) The method of claim 50, wherein the intermediate server computer decrypts at least a portion of the first message using a first encryption key common between the first and third computers to create an unencrypted portion, and then re-encrypts the unencrypted portion using a second encryption key common between the second and third computers, wherein the first and second encryption keys are different.

52. (previously presented) The method of claim 47, further comprising the steps of:

(4) receiving a third HTTP message containing information intended for delivery to the first computer, wherein the third message is received through the firewall associated with the second computer through the port that is normally open by default to Internet traffic; and

(5) transmitting contents of the third message to the first computer over a return path previously established between the first computer and the third computer.

53. (previously presented) The method of claim 47, further comprising the step of, when no message has been received from the first computer for delivery to the second computer, periodically transmitting to the second computer via the return path a message to avoid a time-out condition on the second computer.

54. (previously presented) The method of claim 47, further comprising the step of authenticating that the first computer is authorized to communicate with the second computer prior to step (3).

55. (previously presented) A method of communicating between computers, comprising the steps of:

(1) transmitting from a first computer to an intermediate server computer a first HTTP POST message through a firewall port that is normally open to Internet traffic, wherein the first HTTP POST message requests establishment of a connection between the first computer and the intermediate server computer over a first return path;

(2) receiving from the intermediate server computer a response including a connection

identifier corresponding to the first return path;

(3) periodically transmitting from the intermediate server computer to the first computer a "keep alive" message if no further messages are received from the first computer within a period of time;

(4) exchanging encryption keys between the first computer and the intermediate server computer;

(5) repeating steps (1) through (4) between a second computer and the intermediate server computer, thereby creating a second return path between the second computer and the intermediate server computer;

(6) transmitting encrypted information from the first computer to the intermediate server computer using further HTTP POST messages over the first return path; and

(7) transmitting the encrypted information from the intermediate server over the second return path.

56. (previously presented) The method of claim 55, further comprising the steps of, in the intermediate server computer, decrypting encrypted information received from the first computer using encryption keys shared between the first computer and the intermediate computer, and then re-encrypting the received information using encryption keys shared between the intermediate computer and the second computer.

57. (new) A method of communicating between a first computer protected by a first firewall and a second computer protected by a different second firewall, comprising the steps of:

(1) at a third computer situated between the first firewall and the different second firewall, receiving a first HTTP message from the first computer through a port in the first firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic;

(2) from the third computer, sending a first response message to the first computer through the port in the first firewall, thereby establishing a first receive channel through the first firewall, wherein the first response message is linked to the first HTTP message;

(3) at the third computer, receiving a second HTTP message from the second computer

through a port in the different second firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic;

(4) from the third computer, sending a second response message to the second computer through the port in the different second firewall, thereby establishing a second receive channel through the second firewall, wherein the second response message is linked to the second HTTP message;

(5) at the third computer, receiving a third encrypted HTTP message from the first computer through the port in the first firewall; determining that the third encrypted HTTP message is intended to be delivered to the second computer, and transmitting to the second computer the third encrypted HTTP message, wherein the third encrypted HTTP message is transmitted over the second receive channel to the second computer; and

(6) from the third computer, periodically transmitting "keep alive" messages to the first and second computers to avoid a time-out condition.

58. (new) The method of claim 57, wherein step (5) is performed at the third computer by transmitting the third encrypted HTTP message to the second computer without decrypting contents of the third encrypted HTTP message.